多項式の根を求めるアルゴリズム

情報数理学特別講義I 第11回

2025-11-07

BCH符号の誤り訂正手順と今回の講義内容

以下の3つの手順

1. シンドローム計算
2. 誤り位置多項式計算
3. 誤り位置多項式の根の計算

これまで，3.に関しては元を直接代入することで計算してきた.
今回はこの計算を効率化するアルゴリズムを紹介する.

具体的には，2誤り訂正BCH符号の復号アルゴリズムとして利用可能な
$GF(2^q)$ 上の2次の多項式の根を計算するアルゴリズムを学ぶ.

本日の流れ

1. トレース関数 Tr
2. 線形化多項式 (Linearized Polynomial)
3. $GF(2^q)$ 上の多項式の求根

トレース関数

$GF(p^q)$ 上の 元 a のトレース関数 Tr は,

$$\mathrm{Tr}(a) = a + a^p + a^{p^2} + \cdots + a^{p^{q-1}}$$

で定義される.

任意の $\alpha, \beta \in GF(p^q), c \in GF(p)$ において，トレースは
次の2つの性質を持つ：

- $\mathrm{Tr}(\alpha + \beta) = \mathrm{Tr}(\alpha) + \mathrm{Tr}(\beta)$
- $\mathrm{Tr}(c\alpha) = c\,\mathrm{Tr}(\alpha)$

トレース関数（続き）

先の2つの性質より，$GF(2^q)$ 上の標準基底 $\left\{1, \alpha, \alpha^2, \cdots, \alpha^{q-1}\right\}$ と $GF(2)$ 上の元 a_i で表される任意の元 $a = \sum_{i=0}^{q-1} a_i \alpha^i$ のトレースは

$$\mathrm{Tr}(a) = \mathrm{Tr}\left(\sum_{i=0}^{q-1} a_i \alpha^i\right) = \sum_{i=0}^{q-1} a_i \,\mathrm{Tr}\left(\alpha^i\right)$$

と計算できる．つまり標準基底 $\left\{1, \alpha, \alpha^2, \cdots, \alpha^{q-1}\right\}$ のうち，$\mathrm{Tr}(\alpha^i)$ が 1 である a_i の和を計算すればよい．

トレース関数（続き）

$GF(p^q)$の元を引数にとり，$GF(p)$の元を返すトレース関数は，
$GF(p^q)$から$GF(p)$への線形変換である．
つまり任意の $\alpha \in GF(p^q)$ に対して，$\mathrm{Tr}(\alpha) \in GF(p)$ である．

練習問題1（8分）

原始多項式 $p(x) = 1 + x + x^4$ で構成される $GF(2^4)$ 上の以下の元のトレースを求めよ.

1. 1
2. α
3. α^2
4. α^3
5. α^4

再掲：$GF(p^q)$ 上の 元 a のトレース関数 Tr は,

$$\mathrm{Tr}(a) = a + a^p + a^{p^2} + \cdots + a^{p^{q-1}}$$

線形化多項式 (Linearized Polynomial)

$GF(2^q)$ 上の多項式 $f(x)$ が $f(x) = \sum_i f_i x^{2^i}$ の形式の時，$f(x)$ を線形化多項式と呼ぶ.

線形化多項式の例：

$$f(x) = f_2 x^4 + f_1 x^2 + f_0 x$$

$GF(2^q)$ 上の標準基底 $\left\{1, \alpha, \alpha^2, \cdots, \alpha^{q-1}\right\}$ と $GF(2)$ 上の元 a_i を用いると，任意の整数 k に対して

$$\left(\sum_{i=0}^{q-1} a_i \alpha^i\right)^{2^k} = \sum_{i=0}^{q-1} \left(a_i^{2^k} \left(\alpha^i\right)^{2^k}\right) = \sum_{i=0}^{q-1} \left(a_i \left(\alpha^i\right)^{2^k}\right)$$

が成り立つことから,

※$GF(2^q)$ 上の2乗が容易に計算できたのと同じこと

定理 $f(x)$が線形化多項式のとき，$GF(2^q)$ 上の任意の元 a は標準基底の線形和 $a = \sum_{i=0}^{q-1} a_i \alpha^i$ で表現できることから,

$$f(a) = \sum_{i=0}^{q-1} a_i f(\alpha^i).$$

線形化多項式の評価は線形変換

$$f(a) = \sum_{i=0}^{q-1} a_i f(\alpha^i).$$

より，$f(\alpha^i)$ をあらかじめ計算しておき，q 個の新たな基底とた線形変換操作（$q \times q$ の2元行列との積）により，$f(a)$ が計算できる.

例 $GF(2^4)$ 上の線形化多項式 $f(x) = x^4 + \alpha^5 x^2 + \alpha^7 x$ の計算を考えてみよう．ただし $\alpha \in GF(2^4)$ は 原始多項式 $p(x) = 1 + x + x^4$ の根とする.

$$
\begin{aligned}
f(1) &= \alpha^2 + \alpha^3 \\
f(\alpha) &= 1 + \alpha^2 + \alpha^3 \\
f(\alpha^2) &= 1 + \alpha^2 \\
f(\alpha^3) &= \alpha + \alpha^2
\end{aligned}
$$

よって $f(x)$ の評価に相当する線形変換行列は

$$
F = \begin{pmatrix}
0 & 1 & 1 & 0 \\
0 & 0 & 0 & 1 \\
1 & 1 & 1 & 1 \\
1 & 1 & 0 & 0
\end{pmatrix}.
$$

練習問題2（7分）

$f(x) = x^4 + \alpha^5 x^2 + \alpha^7 x$ の計算が F との積で計算できることを確認してみよう.

1. $f(\alpha^{12})$ を求める.
2. α^{12} のベクトル表記 $\underline{a}$ を用いてを$F\underline{a}$ を計算する.

1.と2.の結果が一致することを確認してください.

再掲：

$$F = \begin{pmatrix} 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 1 & 1 & 1 & 1 \\ 1 & 1 & 0 & 0 \end{pmatrix}.$$

アフィン多項式

$GF(2^q)$ 上の多項式 $f(x)$ が $f(x) = l(x) + u$ の形式の時，$f(x)$ をアフィン多項式と呼ぶ．ただし $l(x)$ は線形化多項式，u は$GF(2^q)$上の定数である．

※線形化多項式は定数項を持たない多項式．アフィン多項式は定数項をもつ多項式．

線形化多項式がバイナリ行列との積で計算できることから，アフィン多項式の根 a は以下の式を満たす元として求められる．

$$L\underline{a} = \underline{u}$$

ただし L は線形化多項式 $l(x)$ の評価に相当する線形変換行列である．

$GF(2^q)$上の2次の多項式の求根

$GF(2^q)$ 上の2次の多項式 $f(x)$ は，$f(x) = f_0 + f_1 x + f_2 x^2$ ただし $f_2 \neq 0$ の形式で表される．$f_1 = 0$ の時，$f(x) = 0$ は $x^2 = f_0 f_2^{-1}$ として計算できる．
$f_1 \neq 0$ のとき，$f(x) = 0$ は $x = f_1 f_2^{-1} y$ で変数変換することにより

$$y^2 + y = f_2 f_0 f_1^{-2}$$

と表現できる．
そしてこの多項式はアフィン多項式の特別なケースとみなすことができ，簡易な計算で根を計算することができる．

アフィン多項式 $y^2 + y = u$ は $\mathrm{Tr}(u) = 0$ のときにのみ根を持つ.
※これは $\mathrm{Tr}(y^2) = \mathrm{Tr}(y)$ であるため，$\mathrm{Tr}(y^2 + y) = 0$ となることからわかる.

いま，α を$GF(2^q)$ の原始元とするとき，α^z を$\mathrm{Tr}(\alpha^z) = 1$ となる適当な元とすると，
アフィン多項式 $y^2 + y = u$ の根を求める変換基底 $y(i) \in GF(2^q)(i = 0, 1, \ldots, q-1)$ を次のように導出することができる.

$$(y(i))^2 + y(i) = \begin{cases} \alpha^i & \text{if } \mathrm{Tr}\left(\alpha^i\right) = 0 \\ \alpha^i + \alpha^z & \text{if } \mathrm{Tr}\left(\alpha^i\right) \neq 0 \end{cases}$$

u を標準基底を用いて $u = \sum_{i=0}^{q-1} u_i \alpha^i$ と表すとき，アフィン多項式の根 y は $y = \sum_{i=0}^{q-1} u_i y(i)$ と計算できる.

なぜならば

$$
\begin{aligned}
y^2 + y &= \left(\sum_{i=0}^{q-1} u_i y(i)\right)^2 + \left(\sum_{i=0}^{q-1} u_i y(i)\right) = \sum_{i=0}^{q-1} u_i y(i)^2 + \sum_{i=0}^{q-1} u_i y(i) \\
&= \sum_{i=0}^{q-1} u_i \left(y(i)^2 + y(i)\right) = \sum_{i=0}^{q-1} u_i \left(\alpha^i + \mathrm{Tr}\left(\alpha^i\right)\alpha^z\right) \\
&= u + \sum_{i=0}^{q-1} u_i \,\mathrm{Tr}\left(\alpha^i\right)\alpha^z \\
&= u + \mathrm{Tr}\left(\sum_{i=0}^{q-1} u_i \alpha^i\right)\alpha^z \\
&= u + \mathrm{Tr}(u)\alpha^z \\
&= u
\end{aligned}
$$

もう一方の根は $y' = y + 1$ で計算される.
$y(i)$ を予め計算しておき，$q \times q$ の2元行列としておくことで，y と y' を簡単に計算することができる.

たとえば，$GF(2^4)$ 上の場合.

$$
\begin{aligned}
y(0) &= \alpha + \alpha^2 \\
y(1) &= 1 + \alpha + \alpha^3 \\
y(2) &= \alpha^3 \\
y(3) &= 1
\end{aligned}
$$

となり,
※$\alpha^z = \alpha^3$ として $y(i)$を求めた.

u から根 y を求める2元行列 Y は

$$Y = \begin{pmatrix} 0 & 1 & 0 & 1 \\ 1 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 \end{pmatrix}$$

となる.

練習問題3

$u = 1 + \alpha^2$ として $y + y^2 + u = 0$ の根を求めてください.

得られた根y, y'を再度上記に代入し，多項式が 0 となるか確かめてください.

2次の誤り位置多項式の根の計算

このように，アフィン多項式の性質を用いて2次の多項式の根が計算できることがわかった．それではいよいよ誤り位置多項式の根を求めてみよう．

$GF(2^4)$ の原始元 α の最小多項式 を $\mu_\alpha(x) = 1 + x + x^4$ とする．生成多項式 $g(x) = \mu_\alpha \mu_{\alpha^3}$ で定義された長さ 15 の2誤り訂正2元BCH符号において，2つの誤りが生じた際の誤り位置多項式は

$$\sigma(x) = \sigma_0 + \sigma_1 x + x^2$$

ただし，$\sigma_0 = \left(S_1^3 - S_3\right) S_1^{-1}, \sigma_1 = S_1$ である．

$$\sigma(x) = \sigma_0 + \sigma_1 x + x^2 = 0$$

の根をもとめるのに，$x = \sigma_1 y$ とすると

$$\sigma_0 + \sigma_1^2 y + \sigma_1^2 y^2 = 0$$
$$\sigma_1^2 (y + y^2) = \sigma_0$$
$$y + y^2 = \sigma_0 \sigma_1^{-2}$$

よって $\mathrm{Tr}(\sigma_0 \sigma_1^{-2}) = 0$ ならば，アフィン多項式 $y^2 + y = \sigma_0 \sigma_1^{-2}$ は根をもち，2元行列Y を使って計算できる.
そして得られた y, y' に対して $x = \sigma_1 y, \sigma_1 y'$ とすることで，$\sigma(x) = 0$ の根が得られる.

$\sigma_0\sigma_1^{-2}$ の計算

$\sigma_0 = \left(S_1^3 - S_3\right)S_1^{-1}, \sigma_1 = S_1$ より

$$\begin{aligned}\sigma_0\sigma_1^{-2} &= \left(S_1^3 - S_3\right)S_1^{-3} \\ &= 1 - S_3S_1^{-3}\end{aligned}$$

で計算すれば良い.

試しに計算してみよう.

第8回の講義スライド p.26 の練習問題4で計算してみる.
$S_1 = \alpha^6, S_3 = \alpha^{13}$ より,

$$u = \sigma_0 \sigma_1^{-2} = 1 - S_3 S_1^{-3} = 1 - \alpha^{13}\alpha^{-18} = 1 - \alpha^{10} = \alpha + \alpha^2$$

$\mathrm{Tr}(\alpha + \alpha^2) = 0$ なので, 根を持つ. よって

$$y = Yu = \begin{pmatrix} 0 & 1 & 0 & 1 \\ 1 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 \end{pmatrix} \begin{pmatrix} 0 \\ 1 \\ 1 \\ 0 \end{pmatrix} = \begin{pmatrix} 1 \\ 1 \\ 0 \\ 0 \end{pmatrix} = 1 + \alpha = \alpha^4$$

$x = S_1 y$ より, $x = \alpha^{10}$ が求まる. また, $y' = y + 1$ より, $x' = \alpha^7$ が求まり, 第8回の講義で求めた根と一致した.

演習

先の計算と同様に，$GF(2^4)$ の原始元 α の最小多項式 を $\mu_\alpha(x) = 1 + x + x^4$ とする．生成多項式 $g(x) = \mu_\alpha \mu_{\alpha^3}$ で定義された長さ 15 の2誤り訂正2元BCH符号によって符号化された多項式を受信し，受信多項式からシンドロームを計算したところ
$S_1 = \alpha^9, S_3 = \alpha^2$ となった.
このとき，誤り位置多項式の根（誤り位置に対応する元）を求めよ.